Advisory Circular

Advisory Material Joint

Subject: System Design and Analysis

Date: 6/10/2002

AC/AMJ No: 25.1309

Initiated By: SDAHWG

Change: Draft
ARSENAL revisied

Table of Contents:

1. PURPOSE.

a. This AC/AMJ describes acceptable means for showing compliance with the requirements of §/JAR 25.1309 of the Federal Aviation Regulations (FAR)/Joint Airworthiness Requirements (JAR). These means are intended to provide guidance to supplement the engineering and operational judgment that must form the basis of any compliance demonstration.

b. The extent to which the more structured methods and guidelines contained in this AC/AMJ should be applied is a function of systems complexity and systems failure consequence. In general, the extent and structure of the analyses required to show compliance with 25.1309 will be greater when the system is more complex and the effects of the failure conditions are more severe. This AC/AMJ is not intended to require that the more structured techniques introduced in this revision be applied where traditional techniques have been shown

to be acceptable for more traditional systems designs. The means described in this AC/AMJ are not mandatory. Other means may be used if they show compliance with §/JAR 25.1309.

2. RESERVED. AC 25.1309-1A dated June 21, 1988/AMJ 25.1309 dated May 11, 1990, is hereby canceled.

3. RELATED DOCUMENTS. The following guidance and advisory materials are referenced herein:

a. Advisory Circulars, Advisory Material Joint.

(1) AMJ 25.1322 Alerting Systems.

(2) AC 25.19/AMJ 25.19 Certification Maintenance Requirements.

(3) AC 20-115B Radio Technical Commission for Aeronautics Document RTCA/DO 178B/ AMJ 20-115B EUROCAE ED-12B.

(4) AC/AMJ 25-901 Safety Assessment of Powerplant Installations.

b. Industry documents.

(1) RTCA, Inc., Document No. DO-160D/EUROCAE ED14D, Environmental Conditions and Test Procedures for Airborne Equipment.

(2) RTCA, Inc., Document No. RTCA/DO-178B/EUROCAE ED12B, Software Considerations in Airborne Systems and Equipment Certification.

(3) Society of Automotive Engineers (SAE) Aerospace Recommended Practice (ARP) 4754/EUROCAE ED-79, Certification Considerations for Highly Integrated or Complex Aircraft Systems.

(4) SAE ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

4. APPLICABILITY OF §/JAR 25.1309. Section/Paragraph 25.1309 is intended as a general requirement that should be applied to any equipment or system be it for type certification, operating rules, or optional, as installed, in addition to specific systems requirements, except as indicated below.

a. While §/JAR 25.1309 does not apply to the performance and flight characteristics of Subpart B and structural requirements of Subparts C and D, it does apply to any system on which compliance with any of those requirements is based. For example, it does not apply to an

airplane's inherent stall characteristics or their evaluation, but it does apply to a stall warning system used to enable compliance with §/JAR 25.207.

b. Single failures or jams covered by JAR 25.671(c)(1) and §/JAR 25.671(c)(3) are excepted from the requirements of §/JAR 25.1309(b)(1)(ii). Section 25.671(c)(1) requires the consideration of single failures, regardless of the probability of the failure. JAR 25.671(c)(1) does not consider the effects of single failures if their probability is shown to be extremely improbable and the failures also meet the requirements of JAR 25.571(a) and (b).

c. Single failures covered by §/JAR 25.735(b)(1) are excepted from the requirements of §/JAR 25.1309(b). The reason concerns the brake system requirement that limits the effect of a single failure to doubling the brake roll stopping distance. This requirement has been shown to provide a satisfactory level of safety without the need to analyze the particular circumstances and conditions under which the single failure occurs.

d. The failure effects covered by §/JAR 25.810(a)(1)(v) and §/JAR 25.812 are excepted from the requirements of §/JAR 25.1309(b). The failure conditions associated with these cabin safety equipment installations are associated with varied evacuation scenarios for which the probability can not be determined. It has not been proven possible to define appropriate scenarios under which compliance with §/JAR 25.1309(b) can be demonstrated. It is therefore considered more practical to require particular design features or specific reliability demonstrations and except these items of equipment from the requirements of §/JAR 25.1309(b). Traditionally, this approach has been found to be acceptable.

e. The requirements of §/JAR 25.1309 are generally applicable to engine, propeller, and propulsion system installations. The specific applicability and exceptions are stated in §/JAR 25.901(c).

f. Some systems and some functions already receive an evaluation to show compliance with specific requirements for specific failure conditions and therefore meet the intent of §/JAR 25.1309 without the need for additional analysis for those specific failure conditions.

5. DEFINITIONS. The following definitions apply to the system design and analysis requirements of §/JAR 25.1309 and the guidance material provided in this AC/AMJ. They should not be assumed to apply to the same or similar terms used in other regulations or ACs/AMJs. Terms for which standard dictionary definitions apply are not defined herein.

a. Analysis. The terms "analysis" and "assessment" are used throughout. Each has a broad definition and the two terms are to some extent interchangeable. However, the term analysis generally implies a more specific, more detailed evaluation, while the term assessment may be a more general or broader evaluation but may include one or more types of analysis. In practice, the meaning comes from the specific application, e.g., fault tree analysis, Markov analysis, Preliminary System Safety Assessment, etc.

b. Assessment. See the definition of analysis above.

c. Average Probability Per Flight Hour. for the purpose of this AC/AMJ, is a representation of the number of times the subject Failure Condition is predicted to occur during the entire operating life of all airplanes of the type divided by the anticipated total operating hours of all airplanes of that type (Note: The Average Probability Per Flight Hour is normally calculated as the probability of a failure condition occuring during a typical flight of mean duration divided by that mean duration).

d. Candidate Certification Maintenance Requirements (CCMR). A periodic maintenance or flight crew check may be used in a safety analysis to help demonstrate compliance with §/JAR 25.1309(b) for Hazardous and Catastrophic Failure Conditions. Where such checks cannot be accepted as basic servicing or airmanship they become Candidate Certification Maintenance Requirements (CCMRs). AC/AMJ 25.19 defines a method by which Certification Maintenance Requirements (CMRs) are identified from the candidates. A CMR becomes a required periodic maintenance check identified as an operating limitation of the type certificate for the airplane.

e. Check. An examination (e.g., an inspection or test) to determine the physical integrity and/or functional capability of an item.

f. Complex. A system is Complex when its operation, failure modes, or failure effects are difficult to comprehend without the aid of analytical methods.

g. Conventional. A system is considered to be Conventional if its functionality, the technological means used to implement its functionality, and its intended usage are all the same as, or closely similar to, that of previously approved systems that are commonly-used.

h. Design Appraisal. This is a qualitative appraisal of the integrity and safety of the system design.

i. Development Assurance. All those planned and systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis.

j. Error. An omission or incorrect action by a crew member or maintenance personnel, or a mistake in requirements, design, or implementation.

k. Event. An occurrence which has its origin distinct from the airplane, such as atmospheric conditions (e.g. gusts, temperature variations, icing and lightning strikes), runway conditions, conditions of communication, navigation, and surveillance services, bird-strike, cabin and baggage fires. The term is not intended to cover sabotage.

l. Failure. An occurrence which affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of function and malfunction). Note: Errors may cause Failures, but are not considered to be Failures.

m. Failure Condition. A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.

n. Installation Appraisal. This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry-accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

o. Latent Failure. A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one which would in combination with one or more specific failures or events result in a Hazardous or Catastrophic Failure Condition.

p. Qualitative. Those analytical processes that assess system and airplane safety in an objective, non-numerical manner.

q. Quantitative. Those analytical processes that apply mathematical methods to assess system and airplane safety.

r. Redundancy. The presence of more than one independent means for accomplishing a given function or flight operation.

s. System. A combination of components, parts, and elements which are inter-connected to perform one or more functions.

6. BACKGROUND.

a. General. For a number of years airplane systems were evaluated to specific requirements, to the "single fault" criterion, or to the fail-safe design concept. As later-generation airplanes developed, more safety-critical functions were required to be performed, which generally resulted in an increase in the complexity of the systems designed to perform these functions. The potential hazards to the airplane and its occupants which could arise in the event of loss of one or more functions provided by a system or that system's malfunction had to be considered, as also did the interaction between systems performing different functions. This has led to the general principle that an inverse relationship should exist between the probability of a Failure Condition and its effect on the airplane and/or its occupants (see Figure 1). In assessing the acceptability of a design it was recognized that rational probability values would have to be established. Historical evidence indicated that the probability of a serious accident due to operational and airframe-related causes was approximately one per million hours of flight. Furthermore, about 10 percent of the total were attributed to Failure Conditions caused by the airplane's systems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new airplane designs. It is reasonable to expect that the probability of a serious accident from all such Failure Conditions be not greater than one per ten million flight hours or 1 x 10-7 per flight hour for a newly designed airplane. The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the

airplane are collectively analyzed numerically. For this reason it was assumed, arbitrarily, that there are about one-hundred potential Failure Conditions in an airplane which could be catastrophic. The target allowable Average Probability per Flight Hour of 1 x 10-7 was thus apportioned equally among these Failure Conditions, resulting in an allocation of not greater than 1 x 10-9 to each. The upper limit for the Average Probability per Flight Hour for Catastrophic Failure Conditions would be 1 x 10-9 which establishes an approximate probability value for the term "Extremely Improbable". Failure Conditions having less severe effects could be relatively more likely to occur.

b. Fail-Safe Design Concept. The Part 25 airworthiness standards are based on, and incorporate, the objectives and principles or techniques of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

(1) The following basic objectives pertaining to failures apply:

(i) In any system or subsystem, the failure of any single element, component, or connection during any one flight should be assumed, regardless of its probability. Such single failures should not be catastrophic.

(ii) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.

(2) The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e. to ensure that Major Failure Conditions are Remote, Hazardous Failure Conditions are Extremely Remote, and Catastrophic Failure Conditions are Extremely Improbable:

(i) Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.

(ii) Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(iii) Isolation and/or Segregation of Systems, Components, and Elements so that the failure of one does not cause the failure of another.

(iv) Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.

(v) Failure Warning or Indication to provide detection.

(vi) Flight crew Procedures specifying corrective action for use after failure detection.

(vii) Checkability: the capability to check a component's condition.

(viii) Designed Failure Effect Limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(ix) Designed Failure Path to control and direct the effects of a failure in a way that limits its safety impact.

(x) Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions.

(xi) Error-Tolerance that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation, and maintenance.

c. Highly Integrated Systems.

(1) A concern arose regarding the efficiency and coverage of the techniques used for assessing safety aspects of highly integrated systems that perform complex and interrelated functions, particularly through the use of electronic technology and software based techniques. The concern is that design and analysis techniques traditionally applied to deterministic risks or to conventional, non-complex systems may not provide adequate safety coverage for more complex systems. Thus, other assurance techniques, such as development assurance utilizing a combination of process assurance and verification coverage criteria, or structured analysis or assessment techniques applied at the airplane level, if necessary, or at least across integrated or interacting systems, have been applied to these more complex systems. Their systematic use increases confidence that errors in requirements or design, and integration or interaction effects have been adequately identified and corrected.

(2) Considering the above developments, as well as revisions made to the §/JAR 25.1309, this AC/AMJ was revised to include new approaches, both qualitative and quantitative, which may be used to assist in determining safety requirements and establishing compliance with these requirements, and to reflect revisions in the rule, considering the whole airplane and its systems. It also provides guidance for determining when, or if, particular analyses or development assurance actions should be conducted in the frame of the development and safety assessment processes. Numerical values are assigned to the probabilistic terms included in the requirements for use in those cases where the impact of system failures is examined by quantitative methods of analysis. The analytical tools used in determining numerical values are intended to supplement, but not replace, qualitative methods based on engineering and operational judgment.

7. FAILURE CONDITION CLASSIFICATIONS AND PROBABILITY TERMS.

a. Classifications. Failure Conditions may be classified according to the severity of their effects as follows:

(1) No Safety Effect: Failure Conditions that would have no effect on safety; for example, Failure Conditions that would not affect the operational capability of the airplane or increase crew workload.

(2) Minor: Failure Conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor Failure Conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some physical discomfort to passengers or cabin crew.

(3) Major: Failure Conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be, for example, a significant reduction in safety margins or functional capabilities, a significant increase in crew workload or in conditions impairing crew efficiency, or discomfort to the flight crew, or physical distress to passengers or cabin crew, possibly including injuries.

(4) Hazardous: Failure Conditions which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be:

(i) A large reduction in safety margins or functional capabilities;

(ii) Physical distress or excessive workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely; or

(iii) Serious or fatal injury to a relatively small number of the occupants other than the flight crew.

(5) Catastrophic: Failure conditions which would result in multiple fatalities, usually with the loss of the airplane. (Note: A "Catastrophic" Failure Condition was defined in previous versions of the rule and the advisory material as a Failure Condition which would prevent continued safe flight and landing.)

b. Qualitative Probability Terms. When using qualitative analyses to determine compliance with §/JAR 25.1309(b), the following descriptions of the probability terms used in §/JAR 25.1309 and this AC/AMJ have become commonly accepted as aids to engineering judgment:

(1) Probable Failure Conditions are those anticipated to occur one or more times during the entire operational life of each airplane.

(2) Remote Failure Conditions are those unlikely to occur to each airplane during its total life, but which may occur several times when considering the total operational life of a number of airplanes of the type.

(3) Extremely Remote Failure Conditions are those not anticipated to occur to each airplane during its total life but which may occur a few times when considering the total operational life of all airplanes of the type.

(4) Extremely Improbable Failure Conditions are those so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of one type.

c. Quantitative Probability Terms. When using quantitative analyses to help determine compliance with §/JAR 25.1309(b), the following descriptions of the probability terms used in this requirement and this AC/AMJ have become commonly accepted as aids to engineering judgment. They are expressed in terms of acceptable ranges for the Average Probability Per Flight Hour.

(1) Probability Ranges.

(i) Probable Failure Conditions are those having an Average Probability Per Flight Hour greater than of the order of 1 x 10-5 .

(ii) Remote Failure Conditions are those having an Average Probability Per Flight Hour of the order of 1x 10-5 or less, but greater than of the order of 1 x 10-7 .

(iii) Extremely Remote Failure Conditions are those having an Average Probability Per Flight Hour of the order of 1x 10-7 or less, but greater than of the order of 1 x 10-9.

(iv) Extremely Improbable Failure Conditions are those having an Average Probability Per Flight Hour of the order of 1x 10-9 or less.

8. SAFETY OBJECTIVE.

a. The objective of §/JAR 25.1309 is to ensure an acceptable safety level for equipment and systems as installed on the airplane. A logical and acceptable inverse relationship must exist between the Average Probability per Flight Hour and the severity of Failure Condition effects, as shown in Figure 1, such that:

(1) Failure Conditions with No Safety Effect have no probability requirement.

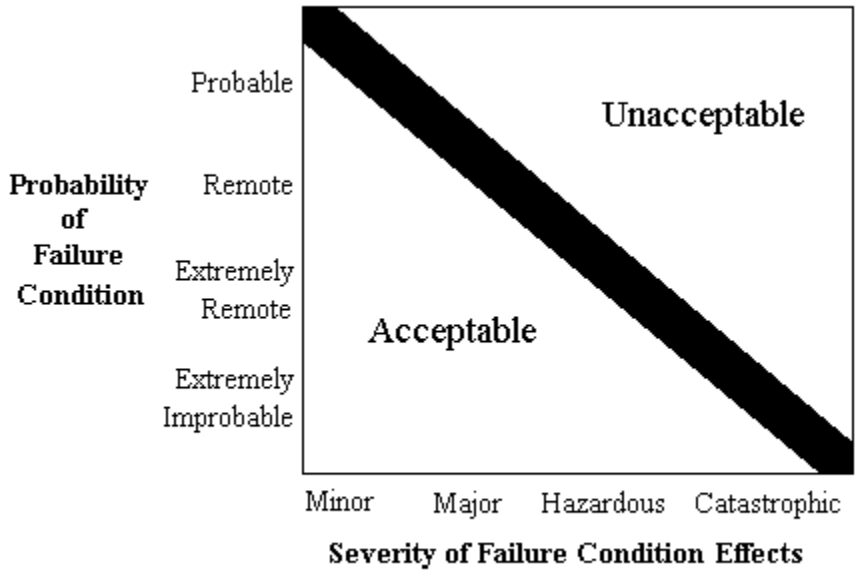
(2) Minor Failure Conditions may be Probable.

(3) Major Failure Conditions must be no more frequent than Remote.

(4) Hazardous Failure Conditions must be no more frequent than Extremely Remote.

(5) Catastrophic Failure Conditions must be Extremely Improbable.

Figure 1: Relationship between Probability and Severity of Failure Condition Effects



b. The safety objectives associated with Failure Conditions are described in Figure 2.

Figure 2: *Relationship Between Probability and Severity of Failure Condition.*

Effect on Airplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote----->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor------>	<-----Major------>	<--Hazardous--->	Catastrophic
Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category airplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

c. The safety objectives associated with Catastrophic Failure Conditions, may be satisfied by demonstrating that:

(1) No single failure will result in a Catastrophic Failure Condition; and

(2) Each Catastrophic Failure Condition is extremely improbable.

d. It is recognized that there could be isolated cases where it may not be practicable to meet the quantitative guidance provided in paragraph 8c (2) for a Catastrophic Failure Condition. Where this is the case, the applicant may propose alternative methods of compliance for FAA concurrence. An acceptable alternative method is to perform all of the following:

(1) Demonstrate that well proven methods for the design and construction of the systems in question have been utilized; and

(2) Determine the average probability per flight hour of each failure condition using structured methods, such as fault tree analysis, markov analysis, or dependency diagrams; and

(3) Demonstrate that the sum of the Average Probabilities per Flight Hour of all Catastrophic Failure Conditions caused by systems is extremely remote (see paragraph 6a for background).

9. COMPLIANCE WITH §/JAR 25.1309. This section describes specific means of compliance for §/JAR 25.1309. The applicant should obtain early concurrence of the certification authority on the choice of an acceptable means of compliance.

a. Compliance with §/JAR 25.1309(a).

(1) Equipment covered by 25.1309(a)(1) must be shown to function properly when installed. The airplane operating and environmental conditions over which proper functioning of the equipment, systems, and installation is required to be considered includes the full normal operating envelope of the airplane as defined by the Airplane Flight Manual together with any modification to that envelope associated with abnormal or emergency procedures. Other external environmental conditions such as atmospheric turbulence, HIRF, lightning, and precipitation, which the airplane is reasonably expected to encounter, should also be considered. The severity of the external environmental conditions which should be considered are limited to those established by certification standards and precedence.

(2) In addition to the external operating and environmental conditions, the effect of the environment within the airplane should be considered. These effects should include vibration and acceleration loads, variations in fluid pressure and electrical power, fluid or vapor contamination, due either to the normal environment or accidental leaks or spillage and handling by personnel. Document referenced in paragraph 3b(1) defines a series of standard environmental test conditions and procedures which may be used to support compliance. Equipment covered by (Joint) Technical Standard Orders containing environmental test procedures or equipment qualified to other environmental test standards can be used to support compliance. The conditions under which the installed equipment will be operated should be equal to or less severe than the environment for which the equipment is qualified.

(3) The required substantiation of the proper functioning of equipment, systems, and installations under the operating and environmental conditions approved for the airplane may be shown by test and/or analysis or reference to comparable service experience on other airplanes. It must be shown that the comparable service experience is valid for the proposed installation. For the equipment systems and installations covered by §/JAR 25.1309(a)(1), the compliance demonstration should also confirm that the normal functioning of such equipment, systems, and installations does not interfere with the proper functioning of other equipment, systems, or installations covered by §/JAR 25.1309(a)(1).

(4) The equipment, systems, and installations covered by §/JAR 25.1309(a)(2) are typically those associated with amenities for passengers such as passenger entertainment

systems, in-flight telephones, etc., whose failure or improper functioning in itself should not affect the safety of the airplane. Operational and environmental qualification requirements for those equipment, systems, and installations are reduced to the tests that are necessary to show that their normal or abnormal functioning does not adversely affect the proper functioning of the equipment, systems, or installations covered by §/JAR 25.1309 (a) (1) and does not otherwise adversely influence the safety of the aircraft or its occupants. Examples of adverse influences are: fire, explosion, exposing passengers to high voltages, etc.

b. Compliance with §/JAR 25.1309(b). Section/Paragraph 25.1309(b) requires that the airplane systems and associated components, considered separately and in relation to other systems must be designed so that any catastrophic Failure Condition is extremely improbable and does not result from a single failure. It also requires that any hazardous Failure Condition is extremely remote, and that any Major Failure Condition is remote. An analysis should always consider the application of the Fail-Safe design concept described in Paragraph 6c, and give special attention to ensuring the effective use of design techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel or more than one system performing operationally similar functions.

(1) General. Compliance with the requirements of §/JAR 25.1309(b) should be shown by analysis and, where necessary, by appropriate ground, flight, or simulator tests. Failure Conditions should be identified and their effects assessed. The maximum allowable probability of the occurrence of each Failure Condition is determined from the Failure Condition's Effects, and when assessing the probabilities of Failure Conditions appropriate analysis considerations should be accounted for. Any analysis must consider:

(i) Possible Failure Conditions and their causes, modes of failure, and damage from sources external to the system.

(ii) The possibility of multiple failures and undetected failures.

(iii) The possibility of requirement, design and implementation errors.

(iv) The effect of reasonably anticipated crew errors after the occurrence of a failure or Failure Condition.

(v) The effect of reasonably anticipated errors when performing maintenance actions.

(vi) The crew alerting cues, corrective action required, and the capability of detecting faults.

(vii) The resulting effects on the airplane and occupants, considering the stage of flight and operating and environmental conditions.

(2) Planning. This AC/AMJ provides guidance on methods of accomplishing the safety objective. The detailed methodology needed to achieve this safety objective will depend on many

factors, in particular the degree of systems complexity and integration. For airplanes containing many complex or integrated systems, it is likely that a plan will need to be developed to describe the intended process. This plan should include consideration of the following aspects:

(i) Functional and physical interrelationships of systems.

(ii) Determination of detailed means of compliance, which may include the use of Development Assurance techniques.

(iii) Means for establishing the accomplishment of the plan.

(3) Availability of Industry Standards and Guidance Materials. There are a variety of acceptable techniques currently being used in industry, which may or may not be reflected in the documents referenced in paragraphs 3b(3) and 3b(4). This AC/AMJ is not intended to constrain the applicant to the use of these documents in the definition of their particular methods of satisfying the objectives of this AC/AMJ. However, these documents do contain material and methods of performing the System Safety Assessment that an applicant may choose to use. These methods, when correctly applied, are recognized by the FAA/JAA as valid for showing compliance with §/JAR 25.1309(b). In addition, the document referenced in paragraph 3b(4) contains tutorial information on applying specific engineering methods (e.g. Markov Analysis, Fault Tree Analysis) that an applicant may wish to utilize in whole or in part.

(4) Acceptable Application of Development Assurance Methods. Paragraph 9b(1)(iii) above requires that any analysis necessary to show compliance with §/JAR 25.1309(b) must consider the possibility of requirement, design, and implementation errors. Errors made during the design and development of systems have traditionally been detected and corrected by exhaustive tests conducted on the system and its components, by direct inspection, and by other direct verification methods capable of completely characterizing the performance of the system. These direct techniques may still be appropriate for simple systems which perform a limited number of functions and which are not highly integrated with other airplane systems. For more complex or integrated systems, exhaustive testing may either be impossible because all of the system states cannot be determined or impractical because of the number of tests which must be accomplished. For these types of systems, compliance may be shown by the use of Development Assurance. The level of Development Assurance should be determined by the severity of potential effects on the aircraft in case of system malfunctions or loss of functions. Guidelines which may be used for providing Development Assurance are described for systems in the document referenced in paragraph 3b(3), and for software in the documents referenced in paragraph 3a(3) and 3b(2). (There is currently no agreed Development Assurance standard for hardware.) Because these documents were not developed simultaneously, there are differences in the guidelines and terminology that they contain. A significant difference is the guidance provided on the use of system architecture for determination of the appropriate development assurance level for hardware and software. The FAA/JAA recognize that consideration of system architecture for this purpose is appropriate. Where apparent differences exist between these documents on this subject, the guidance contained in Appendix D of the document referenced in paragraph 3b(3) should be followed. If the criteria of the document referenced in paragraph

3b(3) are not satisfied by a particular development assurance process the development assurance levels may have to be increased using the guidance of the document referenced in paragraph 3b(2).

(5) Crew and Maintenance Actions.

(i) Where an analysis identifies some indication to, and/or action by, the flight crew, cabin crew, or maintenance personnel, the following activities should be accomplished:

1 Verify that any identified indications are actually provided by the system.

2 Verify that any identified indications will, in fact, be recognized.

3 Verify that any actions required have a reasonable expectation of being accomplished successfully and in a timely manner.

(ii) These verification activities should be accomplished by consulting with engineers, pilots, flight attendants, maintenance personnel and human factors specialists as appropriate, taking due consideration of the consequences if the assumed action is not performed or misperformed.

(iii) In complex situations, the results of the review by specialists may need to be confirmed by simulator or flight tests. However, quantitative assessments of the probabilities of crew or maintenance errors are not currently considered feasible. If the failure indications are considered to be recognizable and the required actions do not cause an excessive workload, then for the purposes of the analysis, the probability that the corrective action will be accomplished, can be considered to be one. If the necessary actions cannot be satisfactorily accomplished, the tasks and/or the systems need to be modified.

c. Compliance with §/JAR 25.1309(c). Section/JAR 25.1309(c) requires that information concerning unsafe system operating conditions must be provided to the crew to enable them to take appropriate corrective action. Compliance with this requirement is usually demonstrated by the analysis identified in Paragraph 9b(1) above, which also includes consideration of crew alerting cues, corrective action required, and the capability of detecting faults. Section/JAR 25.1309(c) requires that a warning indication must be provided if immediate corrective action is required. Section 25.1309(c) further requires that systems and controls, including indication and annunciation, must be designed to minimize crew errors that could create additional hazards. The required information may be provided by dedicated indication and/or annunciation whose forms and functions meet the requirements of § 25.1322 (“Warning, caution, and advisory lights”) or made apparent by the inherent airplane responses. The required information will depend on the degree of urgency for recognition and corrective action by the crew.

(1) Acceptable crew awareness means may be, but not limited to, the following:

(i) A warning, if immediate recognition and corrective or compensatory action by the crew is required;

(ii) A caution, if immediate flightcrew awareness is required and subsequent crew action will be required;

(iii) An advisory, if flightcrew awareness is required and subsequent crew action may be required; or

(iv) Other appropriate forms, such as a message, for other cases.

(2) When failure monitoring and indication are provided by a system, its reliability should be compatible with the safety objectives associated with the system function for which it provides that indication. For example, if the effects of having a failure and not annunciating that failure are Catastrophic, the combination of the failure with the failure of its annunciation must be Extremely Improbable. In addition, unwanted operation (e.g., nuisance warnings) should be assessed. The failure monitoring and indication should be reliable, technologically feasible and economically practicable. Reliable failure monitoring and indication should utilize current state of the art technology to maximize the probability of detecting and indicating genuine failures while minimizing the probability of falsely detecting and indicating non-existent failures. Any indication should be timely, obvious, clear, and unambiguous.

(3) In the case of airplane conditions requiring immediate crew action, a suitable warning indication must be provided to the crew, if not provided by inherent airplane characteristics. In either case, any warning should be rousing and should occur at a point in a potentially catastrophic sequence where the airplane's capability and the crew's ability still remain sufficient for effective crew action.

(4) Unless they are accepted as normal airmanship, procedures for the crew to follow after the occurrence of failure warning should be described in the approved Airplane Flight Manual (AFM) or AFM revision or supplement.

(5) Even if operation or performance is unaffected or insignificantly affected at the time of failure, information to the crew is required if it is considered necessary for the crew to take any action or observe any precautions. Some examples include reconfiguring a system, being aware of a reduction in safety margins, changing the flight plan or regime, or making an unscheduled landing to reduce exposure to a more severe Failure Condition that would result from subsequent failures or operational or environmental conditions. Information is also required if a failure must be corrected before a subsequent flight. If operation or performance is unaffected or insignificantly affected, information and alerting indications may be inhibited during specific phases of flight where corrective action by the crew is considered more hazardous than no action.

(6) The use of periodic maintenance or flight crew checks to detect significant latent failures when they occur is undesirable and should not be used in lieu of practical and reliable failure monitoring and indications. Where this is not accomplished, the system safety assessment should highlight all those significant latent failures that leave the airplane one failure away from a failure condition classified as catastrophic. These cases should be discussed with the FAA/JAA as early as possible after identification.

Paragraph 12 of this AC provides further guidance on the use of periodic maintenance or flight crew checks. Comparison with similar, previously approved systems is sometimes helpful.

(7) Particular attention should be given to the placement of switches or other control devices, relative to one another, so as to minimize the potential for inadvertent incorrect crew action, especially during emergencies or periods of high workload. Extra protection, such as the use of guarded switches, may sometimes be needed.

10. IDENTIFICATION OF FAILURE CONDITIONS AND CONSIDERATIONS WHEN ASSESSING THEIR EFFECTS.

a. Identification of Failure Conditions. Failure Conditions should be identified by considering the potential effects of failures on the airplane and occupants. These should be considered from two perspectives:

(1) by considering failures of airplane level functions - Failure Conditions identified at this level are not dependent on the way the functions are implemented and the systems' architecture.

(2) by considering failures of functions at the system level - these Failure Conditions are identified through examination of the way that functions are implemented and the systems' architectures.

It should be noted that a Failure Condition may result from a combination of lower level Failure Conditions. This requires that the analysis of complex, highly integrated systems, in particular, should be conducted in a highly methodical and structured manner to ensure that all significant Failure Conditions which arise from multiple failures and combinations of lower level Failure Conditions are properly identified and accounted for. The relevant combinations of failures and Failure Conditions should be determined by the whole safety assessment process that encompasses the aircraft and system level functional hazard assessments and common cause analyses. The overall effect on the airplane of a combination of individual system Failure Conditions occurring as a result of a common or cascade failure, may be more severe than the individual system effect. For example, Failure Conditions classified as minor or major by themselves may have hazardous effects at an airplane level, when considered in combination.

b. Identification of Failure Conditions Using a Functional Hazard Assessment.

(1) Before an applicant proceeds with a detailed safety assessment, a Functional Hazard Assessment (FHA) of the airplane and system functions to determine the need for and

scope of subsequent analysis should be prepared. This assessment may be conducted using service experience, engineering and operational judgment, and/or a top-down deductive qualitative examination of each function. A Functional Hazard Assessment is a systematic, comprehensive examination of airplane and system functions to identify potential Minor, Major, Hazardous, and Catastrophic Failure Conditions which may arise, not only as a result of malfunctions or failure to function, but also as a result of normal responses to unusual or abnormal external factors. It is concerned with the operational vulnerabilities of systems rather than with a detailed analysis of the actual implementation.

(2) Each system function should be examined with respect to the other functions performed by the system, because the loss or malfunction of all functions performed by the system may result in a more severe failure condition than the loss of a single function. In addition, each system function should be examined with respect to functions performed by other airplane systems, because the loss or malfunction of different but related functions, provided by separate systems may affect the severity of Failure Conditions postulated for a particular system.

(3) The Functional Hazard Assessment is an engineering tool which should be performed early in the design and updated as necessary. It is used to define the high-level airplane or system safety objectives that must be considered in the proposed system architectures. It should also be used to assist in determining the development assurance levels for the systems. Many systems may need only a simple review of the system design by the applicant to determine the hazard classification. A Functional Hazard Assessment requires experienced engineering judgment and early coordination between the applicant and the certification authority.

(4) Depending on the extent of functions to be examined and the relationship between functions and systems, different approaches to Functional Hazard Assessment may be taken. Where there is a clear correlation between functions and systems, and where system, and hence function, interrelationships are relatively simple, it may be feasible to conduct separate Functional Hazard Assessments for each system, providing any interface aspects are properly considered and are easily understood. However, where system and function interrelationships are more complex, a top down approach, from an airplane level perspective, should be taken in planning and conducting Functional Hazard Assessments.

c. Considerations When Assessing Failure Condition Effects. The requirements of §/JAR 25.1309(b) are intended to ensure an orderly and thorough evaluation of the effects on safety of foreseeable failures or other events, such as errors or external circumstances, separately or in combination, involving one or more system functions. The interactions of these factors within a system and among relevant systems should be considered. In assessing the effects of a Failure Condition, factors which might alleviate or intensify the direct effects of the initial Failure Condition should be considered. Some of these factors include consequent or related conditions existing within the airplane which may affect the ability of the crew to deal with direct effects, such as the presence of smoke, acceleration effects, interruption of communication, interference with cabin pressurization, etc. When assessing the consequences of a given Failure Condition, account should be taken of the failure information provided, the complexity of the crew action, and the relevant crew training. The number of overall Failure

Conditions involving other than instinctive crew actions may influence the flight crew performance that can be expected. Training recommendations may need to be identified in some cases.

(1) The severity of failure conditions should be evaluated according to the following:

(i) Effects on the airplane, such as reductions in safety margins, degradation in performance, loss of capability to conduct certain flight operations, reduction in environmental protection, or potential or consequential effects on structural integrity.

(ii) Effects on the crew members, such as increases above their normal workload that would affect their ability to cope with adverse operational or environmental conditions or subsequent failures.

(iii) Effects on the occupants, i.e., passengers and crew members.

(2) For convenience in conducting design assessments, Failure Conditions may be classified according to the severity of their effects as No Safety Effect, Minor, Major, Hazardous, or Catastrophic. Paragraph 7a above provides accepted definitions of these terms.

(i) The classification of Failure Conditions does not depend on whether or not a system or function is the subject of a specific requirement or regulation. Some "required" systems, such as transponders, position lights, and public address systems, may have the potential for only Minor Failure Conditions. Conversely, other systems which are not "required", such as autoflight systems, may have the potential for Major, Hazardous, or Catastrophic Failure Conditions.

(ii) Regardless of the types of assessment used, the classification of Failure Conditions should always be accomplished with consideration of all relevant factors; e.g., system, crew, performance, operational, external. Examples of factors include the nature of the failure modes, any effects or limitations on performance, and any required or likely crew action. It is particularly important to consider factors that would alleviate or intensify the severity of a Failure Condition. An example of an alleviating factor would be the continued performance of identical or operationally similar functions by other systems not affected by the Failure Condition. Examples of intensifying factors would include unrelated conditions that would reduce the ability of the crew to cope with a Failure Condition, such as weather or other adverse operational or environmental conditions.

11. ASSESSMENT OF FAILURE CONDITION PROBABILITIES AND ANALYSIS CONSIDERATIONS. After the applicant has identified the Failure Conditions and assessed the severity of the effects of Failure Conditions, it is the applicant's responsibility to determine how to show compliance with the requirement and obtain the concurrence of the Certification Authority. Design and installation reviews, analyses, flight tests, ground tests, simulator tests, or other approved means may be used.

a. Assessment of Failure Condition Probabilities.

(1) The probability that a Failure Condition would occur may be assessed as Probable, Remote, Extremely Remote, or Extremely Improbable. These terms are defined in paragraph 7. Each Failure Condition should have a probability that is inversely related to the severity of its effects as described in paragraph 8.

(2) When a system provides protection from events (e.g., cargo compartment fire, gusts), its reliability should be compatible with the safety objectives necessary for the failure condition associated with the failure of the protection system and the probability of such events. (See paragraph 11g this AC/AMJ and Appendix 4.)

(3) An assessment to identify and classify Failure Conditions is necessarily qualitative. On the other hand, an assessment of the probability of a Failure Condition may be either qualitative or quantitative. An analysis may range from a simple report that interprets test results or compares two similar systems to a detailed analysis that may or may not include estimated numerical probabilities. The depth and scope of an analysis depends on the types of functions performed by the system, the severity of Failure Conditions, and whether or not the system is complex.

(4) Experienced engineering and operational judgment should be applied when determining whether or not a system is complex. Comparison with similar, previously-approved systems is sometimes helpful. All relevant systems attributes should be considered; however, the complexity of the software and hardware need not be a dominant factor in the determination of complexity at the system level, e.g., the design may be very complex, such as a satellite communication system, but its function may be fairly simple..

b. Single Failure Considerations.

(1) According to the requirements of §/JAR 25.1309b(1)(ii), a catastrophic failure condition must not result from the failure of a single component, part, or element of a system. Failure containment should be provided by the system design to limit the propagation of the effects of any single failure to preclude catastrophic failure conditions. In addition, there must be no common cause failure which could affect both the single component, part, or element, and its failure containment provisions. A single failure includes any set of failures which cannot be shown to be independent from each other. Appendix 1 and the document referenced in paragraph 3b(4) describe types of common cause analyses which may be conducted to assure that independence is maintained. Failure containment techniques available to establish independence may include partitioning, separation, and isolation.

(2) While single failures must normally be assumed to occur, there are cases where it is obvious that, from a realistic and practical viewpoint, any knowledgeable, experienced person would unequivocally conclude that a failure mode simply would not occur, unless it is associated with a wholly unrelated failure condition that would itself be catastrophic. Once identified and accepted, such cases need not be considered failures in the context of §/JAR 25.1309. For example, with simply loaded static elements, any failure mode resulting from

fatigue fracture can be assumed to be prevented if this element is shown to meet the damage tolerance requirements of §/JAR 25.571.

c. Common Cause Failure Considerations. An analysis should consider the application of the fail-safe design concept described in paragraph 6b and give special attention to ensure the effective use of design and installation techniques that would prevent single failures or other events from damaging or otherwise adversely affecting more than one redundant system channel, more than one system performing operationally similar functions, or any system and an associated safeguard. When considering such common-cause failures or other events, consequential or cascading effects should be taken into account. Some examples of such potential common cause failures or other events would include rapid release of energy from concentrated sources such as uncontained failures of rotating parts (other than engines and propellers) or pressure vessels, pressure differentials, non-catastrophic structural failures, loss of environmental conditioning, disconnection of more than one subsystem or component by overtemperature protection devices, contamination by fluids, damage from localized fires, loss of power supply or return (e.g. mechanical damage or deterioration of connections), excessive voltage, physical or environmental interactions among parts, errors, or events external to the system or to the airplane (see the document referenced in paragraph 3b(4)).

d. Depth of Analysis. The following identifies the depth of analysis expected based on the classification of a failure condition.

(1) No Safety Effect Failure Conditions. A Functional Hazard Assessment, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these Failure Conditions. If the applicant chooses not to do an FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

(2) Minor Failure Conditions. A Functional Hazard Assessment, with a design and installation appraisal, to establish independence from other functions is necessary for the safety assessment of these Failure Conditions. Combinations of failure condition effects, as noted in section 10 above, must also be considered. If the applicant chooses not to do an FHA, the safety effects may be derived from the design and installation appraisal performed by the applicant.

(3) Major Failure Conditions. Major Failure Conditions must be Remote:

(i) If the system is similar in its relevant attributes to those used in other airplanes and the effects of failure would be the same, then design and installation appraisals (as described in Appendix 1), and satisfactory service history of the equipment being analyzed, or of similar design, will usually be acceptable for showing compliance.

(ii) For systems that are not complex, where similarity cannot be used as the basis for compliance, then compliance may be shown by means of a qualitative assessment which shows that the system level Major Failure Conditions, of the system as installed, are consistent with the FHA and are Remote, e.g., redundant systems.

(iii) For complex systems without redundancy, compliance may be shown as in 11d(3)(ii) of this AC/AMJ. To show that malfunctions are indeed Remote in systems of high complexity without redundancy (for example, a system with a self-monitoring microprocessor), it is sometimes necessary to conduct a qualitative functional Failure Modes and Effects Analysis (FMEA) supported by failure rate data and fault detection coverage analysis..

(iv) An analysis of a redundant system is usually complete if it shows isolation between redundant system channels and satisfactory reliability for each channel. For complex systems where functional redundancy is required, a qualitative FMEA and qualitative fault tree analysis may be necessary to determine that redundancy actually exists (e.g. no single failure affects all functional channels).

(4) Hazardous and Catastrophic Failure Conditions. Hazardous Failure Conditions must be Extremely Remote, and Catastrophic Failure Conditions must be Extremely Improbable:

(i) Except as specified in paragraph 11d(4)(ii) below a detailed safety analysis will be necessary for each Hazardous and Catastrophic Failure Condition identified by the functional hazard assessment. The analysis will usually be a combination of qualitative and quantitative assessment of the design.

(ii) For very simple and conventional installations, i.e. low complexity and similarity in relevant attributes, it may be possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote or Extremely Improbable, respectively, on the basis of experienced engineering judgment, using only qualitative analysis. The basis for the assessment will be the degree of redundancy, the established independence and isolation of the channels and the reliability record of the technology involved. Satisfactory service experience on similar systems commonly used in many airplanes may be sufficient when a close similarity is established in respect of both the system design and operating conditions.

(iii) For complex systems where true similarity in all relevant attributes, including installation attributes, can be rigorously established, it may be also possible to assess a Hazardous or Catastrophic Failure Condition as being Extremely Remote or Extremely Improbable, respectively, on the basis of experienced engineering judgment, using only qualitative analysis. A high degree of similarity in both design and application is required to be substantiated.

e. Calculation of Average Probability per Flight Hour (Quantitative Analysis).

(1) The Average Probability per Flight Hour is the probability of occurrence, normalized by the flight time, of a Failure Condition during a flight which can be seen as an average over all possible flights of the fleet of aircraft to be certified. The calculation of the Average Probability per Flight Hour for a Failure Condition should consider

(I) the average flight duration and the average flight profile for the aircraft type to be certified,

(ii) all combinations of failures and events that contribute to the Failure Condition,

(iii) the conditional probability if a sequence of events is necessary to produce the Failure Condition,

(iv) the relevant "at risk" time if an event is only relevant during certain flight phases,

(v) the average exposure time if the failure can persist for multiple flights.

(2) The details how to calculate the Average Probability per Flight Hour for a Failure Condition are given in Appendix 3 of this AC/AMJ.

(3) If the probability of a subject failure condition occuring during a typical flight of mean duration for the airplane type divided by the flight's mean duration in hours is likely to be significantly different from the predicted average rate of occurrance of that failure condition during the entire operational life of all airplanes of that type, then a risk model that better reflects the failure condition should be used.

(4) It is recognized that, for various reasons, component failure rate data are not precise enough to enable accurate estimates of the probabilities of Failure Conditions. This results in some degree of uncertainty, as indicated by the wide line in Figure 1, and the expression "on the order of" in the descriptions of the quantitative probability terms that are provided above. When calculating the estimated probability of each Failure Condition, this uncertainty should be accounted for in a way that does not compromise safety.

f. Integrated Systems. Interconnections between systems have been a feature of airplane design for many years and §/JAR 25.1309(b) recognizes this in requiring systems to be considered in relation to other systems. Providing the interfaces between systems are relatively few and simple, and hence readily understandable, compliance may often be shown through a series of system safety assessments, each of which deals with a particular Failure Condition (or more likely a group of Failure Conditions) associated with a system and, where necessary, takes account of failures arising at the interface with other systems. This procedure has been found to be acceptable in many past certification programs. However, where the systems and their interfaces become more complex and extensive, the task of demonstrating compliance may become more complex. It is therefore essential that the means of compliance are considered early in the design phase to ensure that the design can be supported by a viable safety assessment strategy. Aspects of the guidance material covered elsewhere in this AC/AMJ and which should be given particular consideration are as follows:

(1) planning the proposed means of compliance,

(2) considering the importance of architectural design in limiting the impact and propagation of failures,

(3) the potential for common cause failures and cascade effects and the possible need to assess combinations of multiple lower level (e.g. major) Failure Conditions,

(4) the importance of multi-disciplinary teams in identifying and classifying significant Failure Conditions,

(5) effect of crew and maintenance procedures in limiting the impact and propagation of failures.

In addition, rigorous and well structured design and development procedures play an essential role in facilitating a methodical safety assessment process and providing visibility to the means of compliance. The document referenced in paragraph 3b(3) may be helpful in the certification of highly integrated or complex aircraft systems.

g. Operational or Environmental Conditions. A probability of one should usually be used for encountering a discrete condition for which the airplane is designed, such as instrument meteorological conditions or Category III weather operations. However, Appendix 4 contains allowable probabilities which may be assigned to various operational and environmental conditions for use in computing the average probability per flight hour of failure conditions resulting from multiple independent failures, without further justification. Appendix 4 is provided for guidance and is not intended to be exhaustive or prescriptive. At this time, a number of items have no accepted standard statistical data from which to derive a probability figure. However, these items are included for either future consideration or as items for which the applicant may propose a probability figure supported by statistically valid data or supporting service experience. The applicant may propose additional conditions or different probabilities from those in Appendix 4 provided they are based on statistically valid data or supporting service experience. The applicant should obtain early concurrence of the Certification Authority when such conditions are to be included in an analysis. When combining the probability of such a random condition with that of a system failure, care should be taken to ensure that the condition and the system failure are independent of one another, or that any dependencies are properly accounted for.

h. Justification of Assumptions, Data Sources and Analytical Techniques.

(1) Any analysis is only as accurate as the assumptions, data, and analytical techniques it uses. Therefore, to show compliance with the requirements, the underlying assumptions, data, and analytic techniques should be identified and justified to assure that the conclusions of the analysis are valid. Variability may be inherent in elements such as failure modes, failure effects, failure rates, failure probability distribution functions, failure exposure times, failure detection methods, fault independence, limitation of analytical methods, processes, and assumptions. The justification of the assumptions made with respect to the above items should be an integral part of the analysis. Assumptions can be validated by using experience

with identical or similar systems or components with due allowance made for differences of design, duty cycle and environment. Where it is not possible to fully justify the adequacy of the safety analysis and where data or assumptions are critical to the acceptability of the Failure Condition, extra conservatism should be built into either the analysis or the design. Alternatively any uncertainty in the data and assumptions should be evaluated to the degree necessary to demonstrate that the analysis conclusions are insensitive to that uncertainty.

(2) Where adequate validation data is not available (e.g., new or novel systems), and extra conservatism is built into the analysis, then the normal post-certification in-service follow-up may be performed to obtain the data necessary to alleviate any consequence of the extra conservatism. This data may be used, for example, to extend system check intervals.

12. OPERATIONAL AND MAINTENANCE CONSIDERATIONS. This AC/AMJ addresses only those operational and maintenance considerations that are directly related to compliance with §/JAR 25.1309; other operational and maintenance considerations are not discussed herein. Flight crew and maintenance tasks related to compliance with this requirement should be appropriate and reasonable. However, quantitative assessments of crew errors are not considered feasible. Therefore, reasonable tasks are those for which full credit can be taken because they can realistically be anticipated to be performed correctly when they are required or scheduled. In addition, based on experienced engineering and operational judgment, the discovery of obvious failures during normal operation or maintenance of the airplane may be assumed, even though identification of such failures is not the primary purpose of the operational or maintenance actions. During the safety assessment process associated with § 25.1309 compliance, useful information or instructions associated with the continued airworthiness of the airplane might be identified. This information should be made available to those compiling the Instructions for Continued Airworthiness covered by § 25.1529.

a. Flight crew Action. When assessing the ability of the flight crew to cope with a Failure Condition, the information provided to the crew and the complexity of the required action should be considered. If the evaluation indicates that a potential Failure Condition can be alleviated or overcome without jeopardizing other safety related flight crew tasks and without requiring exceptional pilot skill or strength, credit may be taken for both qualitative and quantitative assessments. Similarly, credit may be taken for correct flight crew performance of the periodic checks required to demonstrate compliance with §/JAR 25.1309(b) provided overall flight crew workload during the time available to perform them is not excessive and they do not require exceptional pilot skill or strength. Unless flight crew actions are accepted as normal airmanship, they should be described in the approved Airplane Flight Manual.

b. Maintenance Action. Credit may be taken for correct accomplishment of reasonable maintenance tasks, for both qualitative and quantitative assessments. The maintenance tasks needed to show compliance with §/JAR 25.1309(b) should be established. In doing this, the following maintenance scenarios can be used:

(1) Annunciated failures will be corrected before the next flight, or a maximum time period will be established before a maintenance action is required. If the latter is acceptable, the analysis should establish the maximum allowable interval before the maintenance

action is required. These maximum allowable intervals should be reflected in either the MMEL or the type certificate.

(2) Latent failures will be identified by a scheduled maintenance task. If this approach is taken, and the Failure Condition is Hazardous or Catastrophic, then a CCMR maintenance task should be established. Some Latent Failures can be assumed to be identified based upon return to service test on the LRU following its removal and repair (component Mean Time Between Failures (MTBF) should be the basis for the check interval time).

c. Candidate Certification Maintenance Requirements.

(1) By detecting the presence of, and thereby limiting the exposure time to significant latent failures that would, in combination with one or more other specific failures or events identified by safety analysis, result in a Hazardous or Catastrophic Failure Condition, periodic maintenance or flight crew checks may be used to help show compliance with §/JAR 25.1309(b). Where such checks cannot be accepted as basic servicing or airmanship they become CCMRs. AC/AMJ 25.19 details the handling of CCMRs.

(2) Rational methods, which usually involve quantitative analysis, or relevant service experience should be used to determine check intervals. This analysis contains inherent uncertainties as discussed in paragraph 11e(3). Where periodic checks become CMRs these uncertainties justify the controlled escalation or exceptional short term extensions to individual CMRs allowed under AC/AMJ 25.19.

d. Flight with Equipment or Functions Known to be Inoperative. An applicant may elect to develop a list of equipment and functions which need not be operative for flight, based on stated compensating precautions that should be taken, e.g., operational or time limitations, flight crew procedures, or ground crew checks. The documents used to show compliance with §/JAR 25.1309, together with any other relevant information, should be considered in the development of this list, which then becomes the basis for a Master Minimum Equipment List (MMEL). Experienced engineering and operational judgment should be applied during the development of the MMEL.

13. ASSESSMENT OF MODIFICATIONS TO PREVIOUSLY CERTIFICATED AIRPLANES. The means to assure continuing compliance with §/JAR 25.1309 for modifications to previously certificated airplanes should be determined on a case by case basis and will depend on the applicable airplane certification basis and the extent of the change being considered. The change could be a simple modification affecting only one system or a major redesign of many systems, possibly incorporating new technologies. The minimal effort for demonstrating compliance to 25.1309 for any modification is an assessment of the impact on the original system safety assessment. The result of this assessment may range from a simple statement that the existing system safety assessment still applies to the modified system in accordance with the original means of compliance, to the need for new means of compliance encompassing the plan referred to in Section 9b. (STC applicants, if the TC holder is unwilling to release or transfer proprietary data in this regard, the STC applicant may have to create the

System Safety Assessment. Further guidance may be found in Section 11 of the document referenced in paragraph 3b(3).)
It is recommended that the appropriate authority be contacted early to obtain agreement on the means of compliance.

APPENDIX 1. ASSESSMENT METHODS. Various methods for assessing the causes, severity, and probability of Failure Conditions are available to support experienced engineering and operational judgment. Some of these methods are structured. The various types of analysis are based on either inductive or deductive approaches. Probability assessments may be qualitative or quantitative. Descriptions of some types of analysis are provided below and in the document referenced in paragraph 3b(4).

a. Design Appraisal. This is a qualitative appraisal of the integrity and safety of the system design.

b. Installation Appraisal. This is a qualitative appraisal of the integrity and safety of the installation. Any deviations from normal, industry accepted installation practices, such as clearances or tolerances, should be evaluated, especially when appraising modifications made after entry into service.

c. Failure Modes and Effects Analysis. This is a structured, inductive, bottom-up analysis which is used to evaluate the effects on the system and the airplane of each possible element or component failure. When properly formatted, it will aid in identifying latent failures and the possible causes of each failure mode. The document referenced in paragraph 3b(4) provides methodology and detailed guidelines which may be used to perform this type of analysis. A FMEA could be a piece part FMEA or a functional FMEA. For modern microcircuit based LRUs and systems an exhaustive piece part FMEA is not practically feasible with the present state of the art. In that context, a FMEA may be more functional than piece part oriented. A functional oriented FMEA can lead to uncertainties in the qualitative and quantitative aspects which can be compensated for by more conservative assessment such as:

-- assuming all failure modes result in the Failure Conditions of interest,

-- careful choice of system architecture,

-- taking into account the experience lessons learned on the use of similar technology,

d. Fault Tree or Dependence Diagram Analysis. Structured, deductive, top-down analyses which are used to identify the conditions, failures, and events that would cause each defined Failure Condition. They are graphical methods of identifying the logical relationship between each particular Failure Condition and the primary element or component failures, other events, or combinations thereof that can cause it. A failure modes and effects analysis may be used as the source document for those primary failures or other events.

e. Markov Analysis. A Markov model (chain) represents various system states and the relationships among them. The states can be either operational or non-operational. The transitions from one state to another is a function of the failure and repair rates. Markov analysis can be used as a replacement for fault tree/dependence diagram analysis, but it often leads to

more complex representation, especially when the system has many states. It is recommended that Markov analysis be used when fault tree or dependence diagrams are not easily usable, namely to take into account complex transition states of systems which are difficult to represent and handle with classical fault tree or dependence diagram analysis.

f. Common Cause Analysis. The acceptance of adequate probability of failure conditions is often derived from the assessment of multiple systems based on the assumption that failures are independent. Therefore, it is necessary to recognize that such independence may not exist in the practical sense and specific studies are necessary to ensure that independence can either be assured or deemed acceptable.

The Common Cause Analysis is sub-divided into three areas of study:

(1) Zonal Safety Analysis. This analysis has the objective of ensuring that the equipment installations within each zone of the airplane are at an adequate safety standard with respect to design and installation standards, interference between systems, and maintenance errors. In those areas of the airplane where multiple systems and components are installed in close proximity, it should be ensured that the zonal analysis will identify any failure or malfunction which by itself is considered sustainable, but which could have more serious effects when adversely affecting other adjacent systems or components.

(2) Particular Risk Analysis. Particular risks are defined as those events or influences which are outside the systems concerned. Examples are fire, leaking fluids, bird strike, tire burst, high intensity radiated fields exposure, lightning, uncontained failure of high energy rotating machines, etc. Each risk should be the subject of a specific study to examine and document the simultaneous or cascading effects or influences which may violate independence.

(3) Common Mode Analysis. This analysis is performed to confirm the assumed independence of the events which were considered in combination for a given failure condition. The effects of specification, design, implementation, installation, maintenance, and manufacturing errors, environmental factors other than those already considered in the particular risk analysis, and failures of system components should be considered.

g. Safety Assessment Process. Appendix 2 provides an overview of the Safety Assessment Process.

APPENDIX 2. SAFETY ASSESSMENT PROCESS OVERVIEW. In showing compliance with 25.1309(b), the considerations covered in this AC/AMJ should be addressed in a methodical and systematic manner which ensures that the process and its findings are visible and readily assimilated. This appendix is provided primarily for the use of applicants who are not familiar with the various methods and procedures generally used in the industry to conduct safety assessments. This guide and Figures A2-1 and A2-2 are not certification checklists, and they do not include all the information provided in this AC/AMJ. There is no necessity for an applicant to use them or for the authority to accept them, in whole or in part, to show compliance with any regulation. Their sole purposes are to assist applicants by illustrating a systematic approach to safety assessments, to enhance understanding and communication by summarizing some of the information provided in this AC/AMJ, and to provide some suggestions on documentation. More detailed guidance can be found in the document referenced in paragraph 3(b)(4). The document referenced in paragraph 3(b)(3) includes additional guidance on how the safety assessment process relates to the system development process.

a. Define the system and its interfaces, and identify the functions that the system is to perform. Determine whether or not the system is complex, similar to systems used on other airplanes, or conventional. Where multiple systems and functions are to be evaluated, consider the relationships between multiple safety assessments.

b. Identify and classify failure conditions. All relevant applicant engineering organizations, such as systems, structures, propulsion, and flight test, should be involved in this process. This identification and classification may be done by conducting a Functional Hazard Assessment, which is usually based on one of the following methods, as appropriate:

(1) If the system is not complex and its relevant attributes are similar to those of systems used on other airplanes, the identification and classification may be derived from design and installation appraisals and the service experience of the comparable, previously approved systems.

(2) If the system is complex, it is necessary to systematically postulate the effects on the safety of the airplane and its occupants resulting from any possible failures, considered both individually and in combination with other failures or events.

c. Choose the means to be used to determine compliance with §/JAR 25.1309. The depth and scope of the analysis depends on the types of functions performed by the system, the severity of system Failure Conditions, and whether or not the system is complex (see Figure A2-2). For Major Failure Conditions, experienced engineering and operational judgment, design and installation appraisals and comparative service experience data on similar systems may be acceptable, either on their own or in conjunction with qualitative analyses or selectively used quantitative analyses. For Hazardous or Catastrophic Failure Conditions, a very thorough safety assessment is necessary. The applicant should obtain early concurrence of the certification authority on the choice of an acceptable means of compliance.

d. Conduct the analysis and produce the data which are agreed with the certification authority as being acceptable to show compliance. A typical analysis should include the following information to the extent necessary to show compliance:

(1) A statement of the functions, boundaries, and interfaces of the system.

(2) A list of the parts and equipment of which the system is comprised, including their performance specifications or design standards and development assurance levels if applicable. This list may reference other documents, e.g., Technical Standard Orders (TSOs), manufacturer's or military specifications, etc.

(3) The conclusions, including a statement of the failure conditions and their classifications and probabilities (expressed qualitatively or quantitatively, as appropriate) that show compliance with the requirements of §/JAR 25.1309.

(4) A description that establishes correctness and completeness and traces the work leading to the conclusions. This description should include the basis for the classification of each failure condition (e.g., analysis or ground, flight, or simulator tests). It should also include a description of precautions taken against common-cause failures, provide any data such as component failure rates and their sources and applicability, support any assumptions made, and identify any required flight crew or ground crew actions, including any CCMRs.

e. Assess the analyses and conclusions of multiple safety assessments to ensure compliance with the requirements for all aircraft level failure conditions.

f. Prepare compliance statements, maintenance requirements, and flight manual requirements.

Figure A2-1: Safety Assessment Process Overview

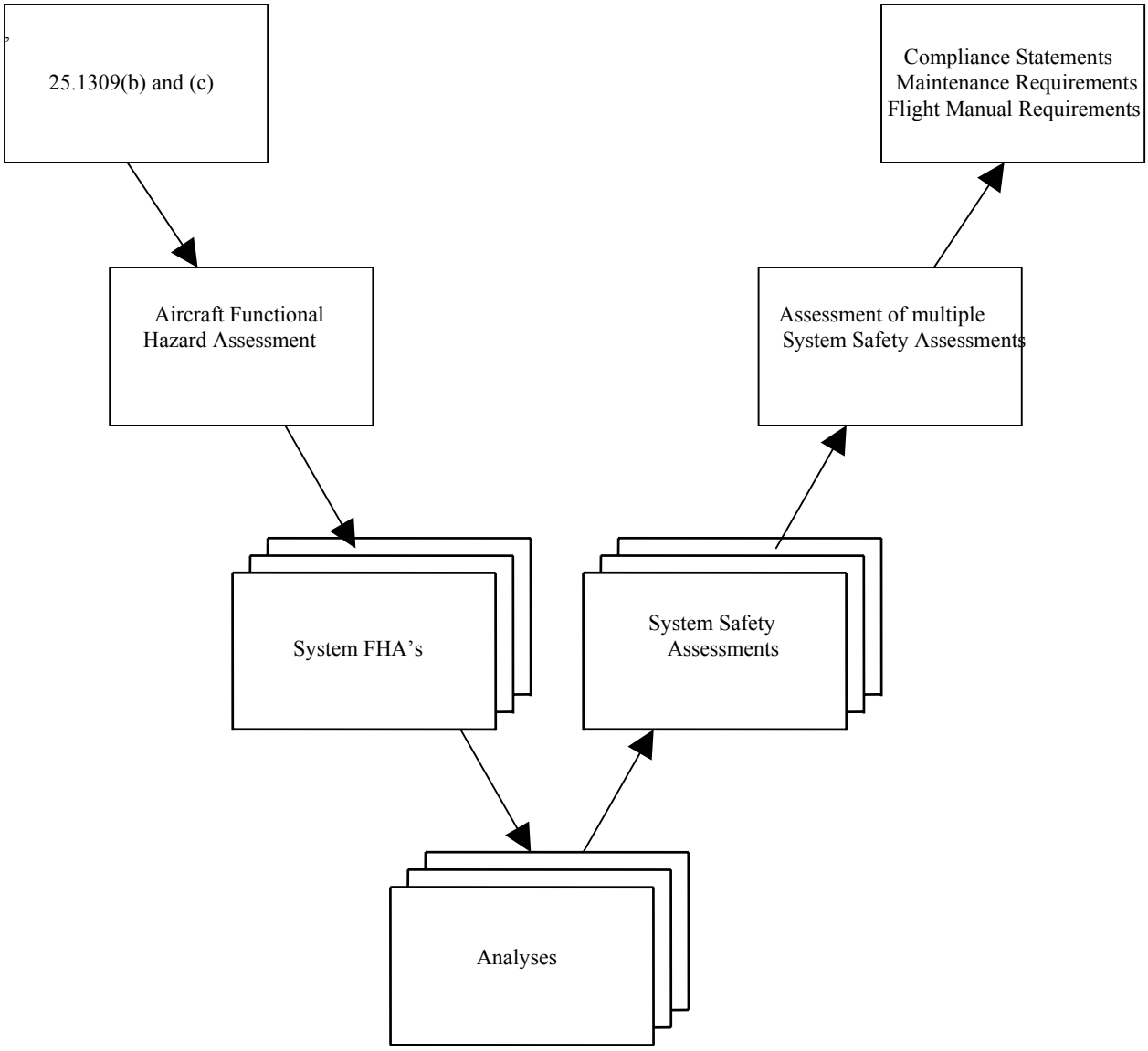
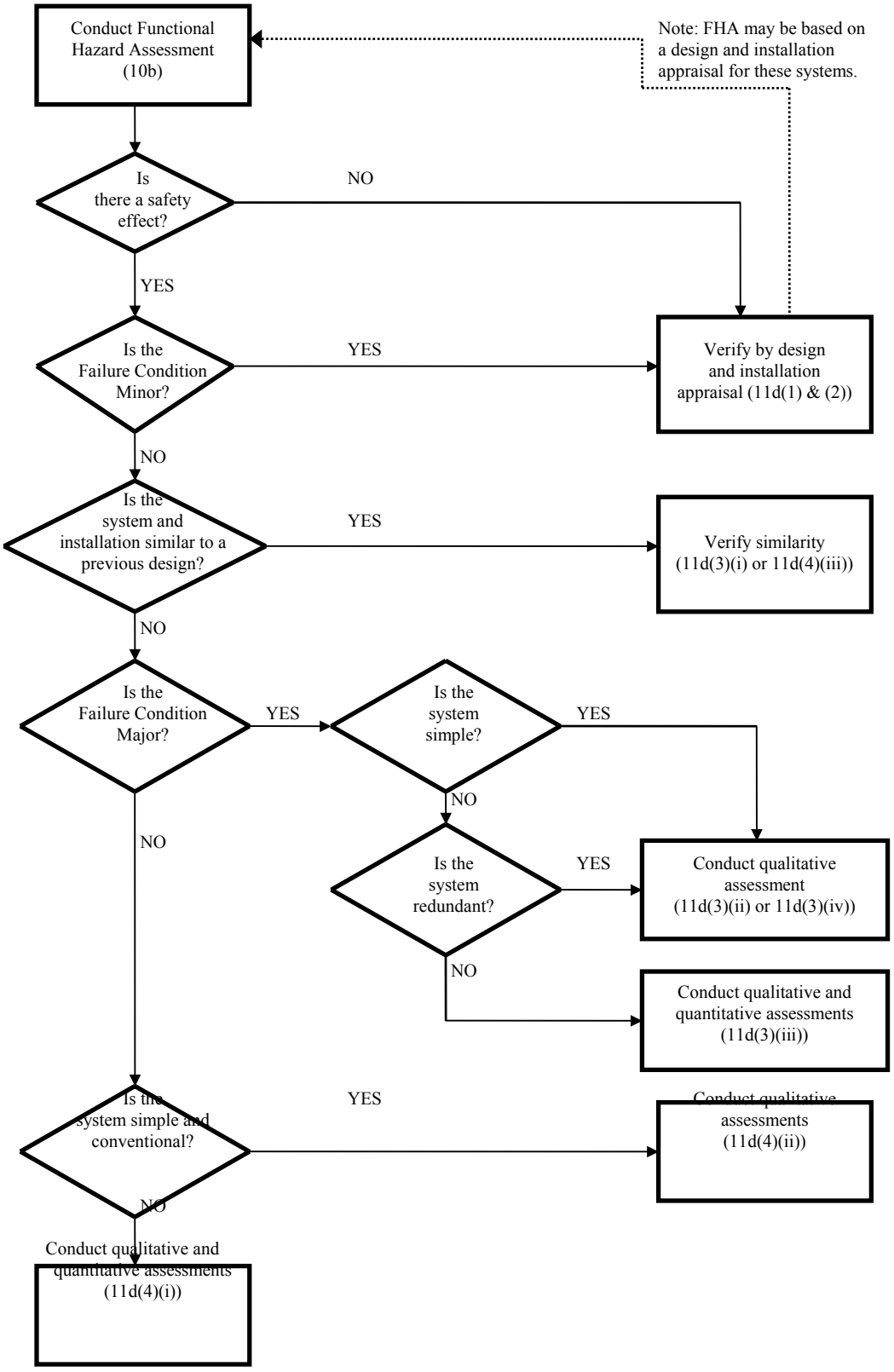


Figure A2-2: Depth of Analysis Flowchart.



APPENDIX 3. CALCULATION OF THE AVERAGE PROBABILITY PER FLIGHT HOUR. The purpose of this material is to provide guidance for calculating the "Average Probability per Flight Hour" for a Failure Condition so that it can be compared with the quantitative criteria of the AC/AMJ.

The process of calculating the "Average Probability per Flight Hour" for a Failure Condition will be described as a four step process and is based on the assumption that the life of an aircraft is a sequence of "Average Flights".

Step 1: Determination of the "Average Flight"

Step 2: Calculation of the probability of a Failure Condition for a certain "Average Flight"

Step 3: Calculation of the "Average Probability per Flight" of a Failure Condition

Step 4: Calculation of the "Average Probability Per Flight Hour" of a Failure Condition

a. Determination of the "Average Flight". The "Average Probability per Flight Hour" is to be based on an "Average Flight". The applicant should estimate the average flight duration and average flight profile for the fleet of aircraft to be certified. The average flight duration should be estimated based on the applicant's expectations and historical experience for similar types. The "Average Flight" duration should reflect the applicants best estimate of the cumulative flight hours divided by the cumulative aircraft flights for the service life of the aircraft. The "Average Flight" profile should be based on the operating weight and performance expectations for the average aircraft when flying a flight of average duration in an ICAO standard atmosphere. The duration of each flight phase (e.g. takeoff, climb, cruise, descent, approach and landing) in the "Average Flight" should be based on the average flight profile. Average taxi times for departure and arrival at an average airport should be considered where appropriate and added to the average flight time. The "Average Flight" duration and profile should be used as the basis for determining the "Average Probability per Flight Hour" for a quantitative safety assessment.

b. Calculation of the Probability of a Failure Condition for a certain "Average Flight" . The probability of a Failure Condition occurring on an "Average Flight" P_{Flight}(Failure Condition) should be determined by structured methods (see the document referenced in paragraph 3b(4) for example methods) and should consider all significant elements (e.g. combinations of failures and events) that contribute to the Failure Condition. The following should be considered:

(1) The individual part, component, and assembly failure rates utilized in calculating the "Average Probability per Flight Hour" should be estimates of the mature constant failure rates after infant mortality and prior to wear-out and should be based on all causes of failure (operational, environmental, etc.). Where available, service history of same or similar components in the same or similar environment should be used.

(2) If the failure is only relevant during certain flight phases, the calculation should be based on the probability of failure during the relevant "at risk" time for the "Average Flight".

(3) If one or more failed elements in the system can persist for multiple flights (latent, dormant, or hidden failures), the calculation should consider the relevant exposure times (e.g. time intervals between maintenance and operational checks/ inspections). In such cases the probability of the Failure Condition increases with the number of flights during the latency period.

(4) If the failure rate of one element varies during different flight phases, the calculation should consider the failure rate and related time increments in such a manner as to establish the probability of the Failure Condition occurring on an "Average Flight":
It is assumed that the "Average Flight" can be divided into n phases (phase 1, ... , phase n). Let T_F the "Average Flight" duration, T_j the duration of phase j and t_j the transition point between T_j and T_{j+1}, j=1, ... ,n . I.e.

$$T_F = \sum_{j=1}^{n} T_j \quad \text{and} \quad t_j - t_{j-1} = T_j \; ; \; j = 1, \ldots, n$$

Let $\lambda_j(t)$ the failure rate function during phase j, i.e. for $t \in [t_{j-1},t_j]$.

Remark: $\lambda_j(t)$ may be equal 0 for all $t \in [t_{j-1},t_j]$ for a specific phase j.

Let $\mathbf{P_{Flight}}$ (Failure) the probability that the element fails during one certain flight (including non-flying time) and $\mathbf{P_{Phase\ j}}$ (Failure) the probability that the element fails in phase j.

Two cases are possible:

(i) The element is checked operative at the beginning of the certain flight. Then

$$P_{Flight}(Failure) = \sum_{j=1}^{n} P_{Phase\ j}(Failure) = \sum_{j=1}^{n} P\left(Failure \,\middle|\, t \in \left[t_{j-1}, t_j\right]\right)$$

$$= 1 - \prod_{i=1}^{n} \exp\left(- \int_{t_{i-1}}^{t_i} \lambda_i(x)\, dx \right)$$

(ii) The state of the item is unknown at the beginning of the certain flight. Then where $\mathbf{P_{prior}}$ (Failure) is the probability that the failure of the element has occurred

$$P_{Flight}(Failure) = P_{prior}(Failure) + \left(1 - P_{prior}(Failure)\right) \cdot \left(1 - \prod_{i=1}^{n} \exp\left(- \int_{t_{i-1}}^{t_i} \lambda_i(x)\, dx \right) \right)$$

prior to the certain flight.

(5) If there is only an effect when failures occur in a certain order, the calculation should account for the conditional probability that the failures occur in the sequence necessary to produce the Failure Condition.

c. Calculation of the Average Probability per Flight of a Failure Condition. The next step is to calculate the "Average Probability per Flight" for the Failure Condition. I.e. the probability of the Failure Condition for each flight (which might be different although all flights are "Average Flights") during the relevant time (e.g. the least common multiple of the exposure times or the aircraft life) should be calculated, summed up and divided by the number of flights during that period. The principles of calculating are described below and also in more detail in Document referenced in paragraph 3b(4).

$$P_{\text{Average per Flight}}(\text{Failure Condition}) = \frac{\sum_{k=1}^{N} P_{\text{Flight k}}(\text{Failure Condition})}{N}$$

Where N is the quantity of all flights during the relevant time, and P_{Flightk} is the probability that the Failure Condition occurs in flight k.

d. Calculation of the Average Probability per Flight Hour of a Failure Condition. Once the "Average Probability per Flight" has been calculated it should be normalized by dividing it by the "Average Flight" duration $\mathbf{T_F}$ in Flight Hours to obtain the "Average Probability per Flight Hour". This quantitative value should be used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant for the Failure Condition being analyzed.

$$P_{\text{Average per FH}}(\text{Failure Condition}) = \frac{P_{\text{Average per Flight}}(\text{Failure Condition})}{T_F}$$

APPENDIX 4. ALLOWABLE PROBABILITIES.
The following probabilities may be used for environmental conditions and operational factors in quantitative safety analyses:

Environmental Factors

Condition	Model or other Justification	Probability
Dispatch into Appendix C Icing		1
Icing outside Appendix C		No Accepted Standard data
Probability of specific icing conditions (largest water droplet, temperature etc) within a given flight		No accepted standard data
Head wind >25 kts during takeoff and landing	AC 120-28 JAR-AWO	10^{-2} per flight
Tail wind >10 kts during takeoff and landing	AC 120-28 JAR-AWO	10^{-2} per flight
Cross wind >20 kts during takeoff and landing	AC 120-28 JAR-AWO	10^{-2} per flight
Limit design gust and turbulence	§/JAR 25.341(Under review by Structures Harmonization Working Group)	10^{-5} per flight hour
Air temperature < -70^{o}C		No accepted standard data
Lightning strike		No accepted standard data
HIRF conditions		No accepted standard data

Aircraft Configurations

Configuration	Model or other Justification	Probability
Center of gravity	Standard industry practice	Uniform over approved range.
Landing and Takeoff Weights/Masses	Standard industry practice	Uniform over approved range.

Flight Conditions

Condition	Model or other Justification	Probability
Flight condition requiring Stall Warning	Assumption	10^{-2} per flight
Flight condition resulting in a Stall	Assumption	10^{-5} per flight
Exceedence of VMO/MMO	Assumption	10^{-2} per flight
Flight condition greater than or equal to 1.5 g		No accepted standard data
Flight condition less than or equal to 0 g		No accepted standard data

Mission Dependencies

Event	Model or other Justification	Probability
Any rejected take-off		No accepted standard data
High energy rejected take-off		No accepted standard data
Need to jettison fuel		No accepted standard data
Go-around		No accepted standard data

Other Events

Event	Model or other Justification	Probability
Fire in a lavatory		No accepted standard data
Fire in a cargo compartment		No accepted standard data
Fire in APU compartment		No accepted standard data
Engine fire		No accepted standard data
Cabin high altitude requiring passenger oxygen		No accepted standard data

If “No accepted standard data” appears in the above tables, the applicant must provide a justified value if a probability less than 1 is to be used in the analysis.

Note: The probabilities quoted in this appendix have been found to be appropriate for use in the context of a quantitative safety analysis performed to demonstrate compliance with FAR/JAR 25.1309. They may not always be appropriate for use in the context of other regulations.